

JEAN-GUILLAUME DUMAS • PASCAL LAFOURCADE
ARIANE TICHIT • SÉBASTIEN VARRETTE

LES BLOCK CHAINS

EN 50 QUESTIONS

Comprendre le fonctionnement
et les enjeux
de cette technologie

DUNOD



JEAN-GUILLAUME DUMAS • PASCAL LAFOURCADE • ETIENNE ROUDEIX
ARIANE TICHIT • SÉBASTIEN VARRETTE



LES NFT

EN 40 QUESTIONS

Des réponses claires et détaillées
pour comprendre
les Non Fungible Tokens



DUNOD



La Blockchain et Web3

Pascal Lafourcade



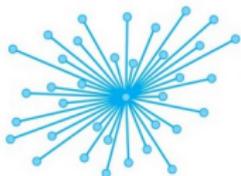
Valence

17 octobre 2023

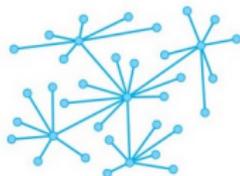
La révolution Bitcoin 2009



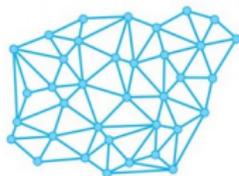
► Crypto-monnaie décentralisée et distribuée



Système centralisé



Système décentralisé



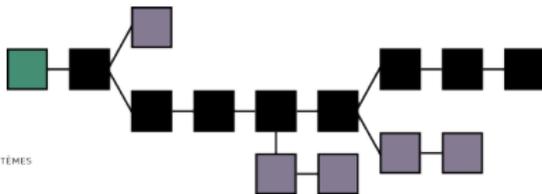
Système distribué



21 millions BTC

► Inarrêtable car distribuée

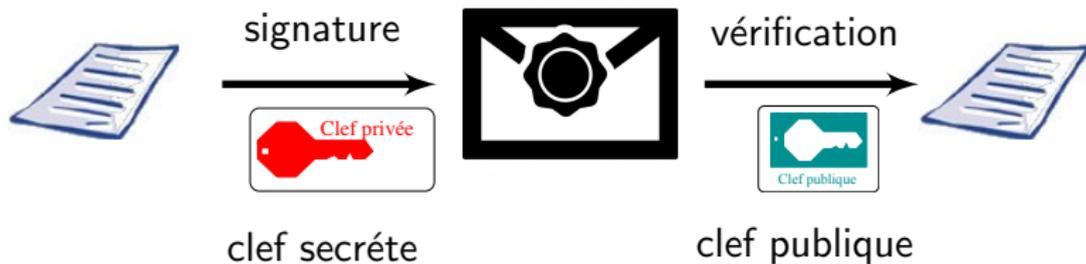
► Infalsifiable et auditable



Taux de change du bitcoin

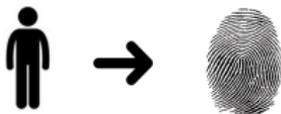


Signature



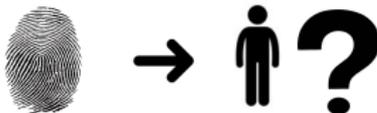
RSA: $m^d \bmod n$

Fonction de Hachage (RIPEMD-160, SHA-256)



Propriétés de résistance

▶ Pré-image



▶ Seconde Pré-image



▶ Collision



Miner des Bitcoins



Miner des Bitcoins



Les “mineurs” valident les transactions contre des bitcoins



Miner des Bitcoins

- ▶ Valider = résoudre un **objectif de hachage**
- ▶ Récompense initiale 50 BTC pour une validation
- ▶ Divisée par 2 tous les 210000 validations

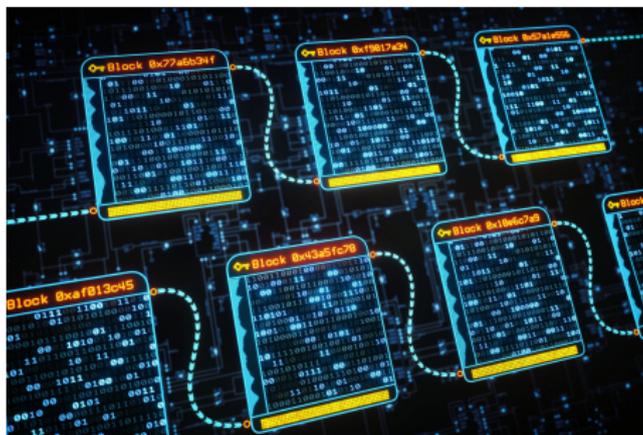
$$\sum_{i=0}^{32} \frac{50}{2^i} \times 210\,000 = 21 \text{ millions BTC}$$



Blockchain

The St Lawrence				Starob Company (Limited)			
Incorporated by Letters Patent				under "The Companies Act"			
Capital \$8000 in				800 Shares of \$100 each.			
Limited				Liability			
First issue of 405				Shares \$40500			
<p>We the undersigned do hereby subscribe in the Capital Stock of the St Lawrence Starob and Co. Ltd and do assign promise and agree to pay the full amount of the said respective shares as shown by this stock book and the balance at such time and in such manner and amount as by the Directors & Provisional Directors of the said Company may be determined.</p>				<p>for the number of shares set opposite our respective names Company (Limited) and we do each for himself and himself to pay the full amount of the said respective shares as shown by this stock book and the balance at such time and in such manner and amount as by the Directors & Provisional Directors of the said Company may be determined.</p>			
Trade	Subscribers	Shares	Residence	No of Shares	Remarks	Witness	Amount
1899 Sept 11th Nov 29 Dec 5	Robt Kilgus Chas. Nicholson Joseph Wilson John Gray Samuel Halperin		Toronto Toronto Toronto Cardinal Cardinal	one Hundred one hundred two one hundred one hundred two one share		Atkinson Atkinson Atkinson Mainway Mainway	\$10,000.00 \$10,200.00 \$10,000.00 \$10,200.00 \$100.00

Blockchain

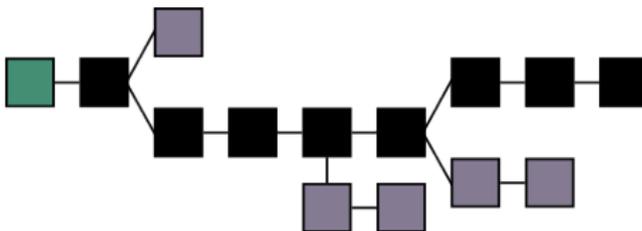


Registre distribué, sécurisé, infalsifiable

Mineurs valident des transactions

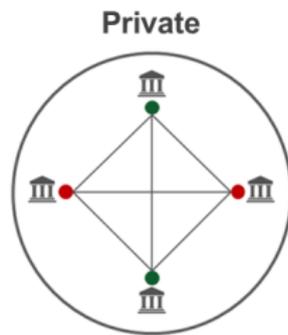
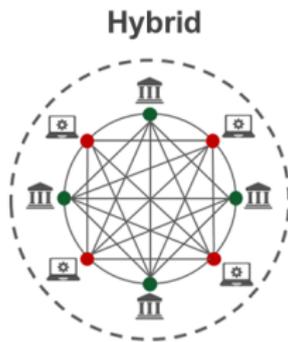
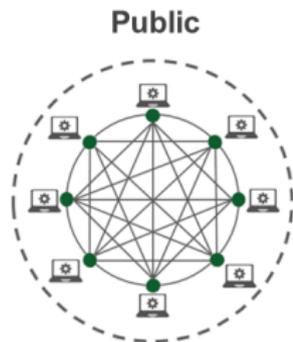


Tiennent à jour le registre distribué

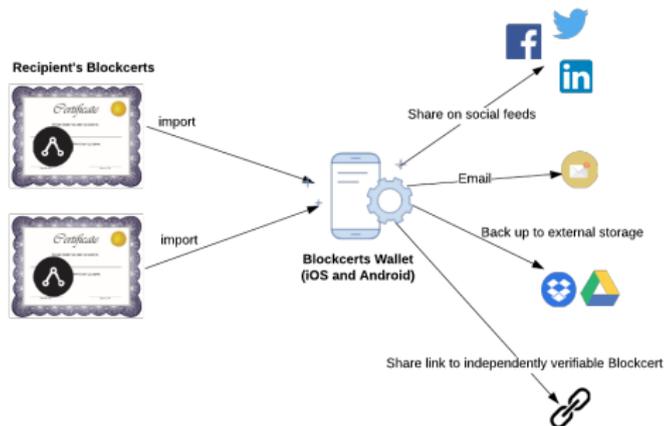


Inarrêtable, Infalsifiable, Auditable

Blockchain Privée vs Publique



Blockchain Application : MIT Diploma



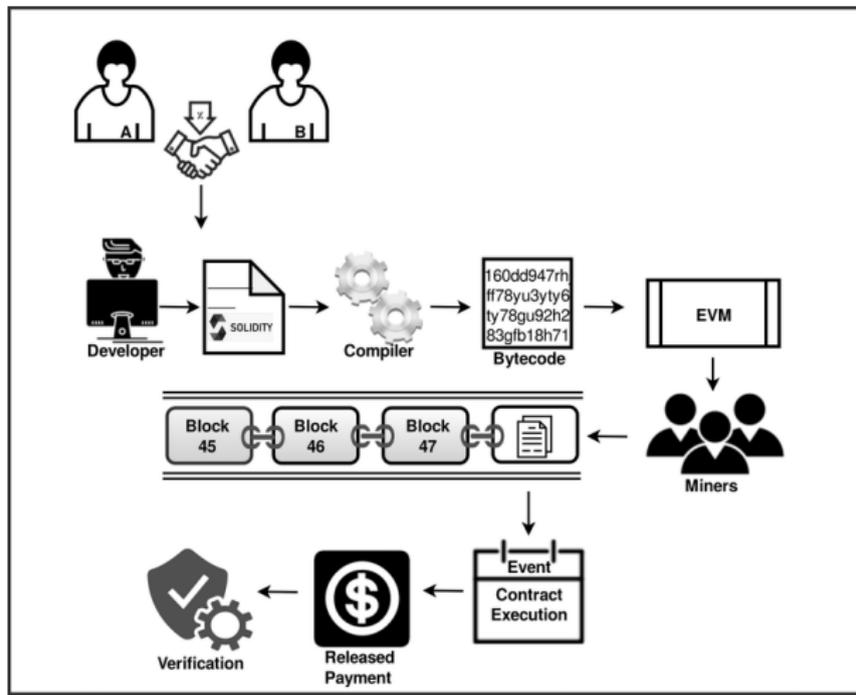
Blockchain Applications : Auction



Properties

Universal Verifiability, Individual Verifiability, Privacy,
Receipt-Freeness, Prevent Double Spending, Non-Repudiation ...

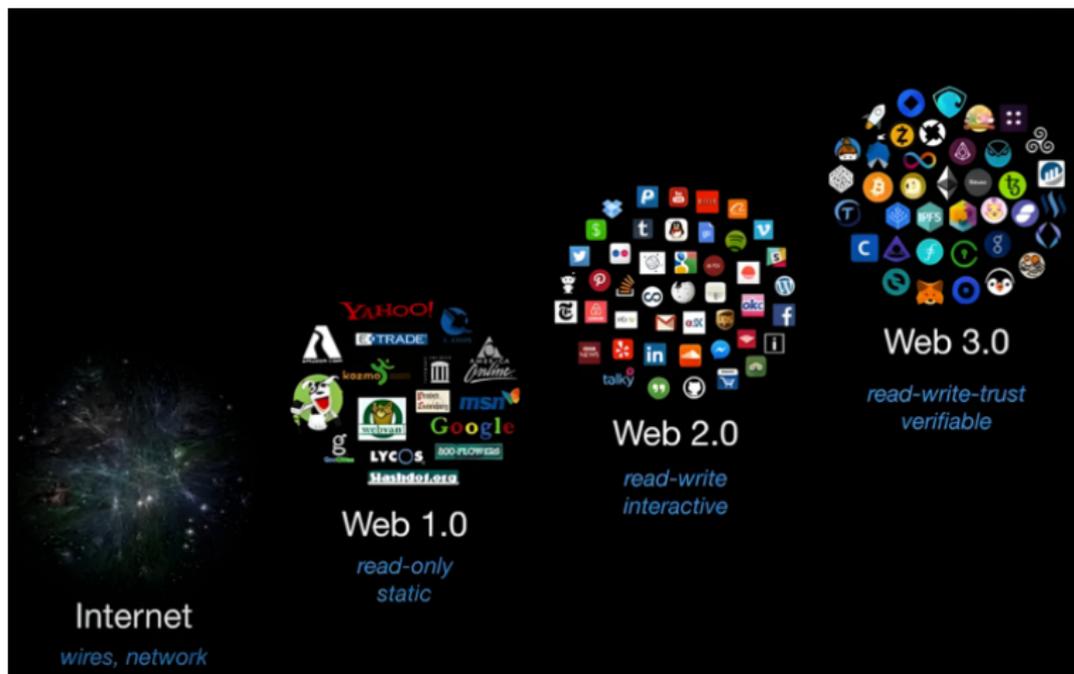
Smart Contract



Smart Contract



Internet to Web3



Choses à retenir

- ▶ La révolution Blockchain est en marche
- ▶ Un formidable outil
- ▶ De nombreuses applications mais bien comprendre les limites
- ▶ La cryptographie est au centre de la sécurité

Merci pour votre attention

Questions ?



pascal.lafourcade@uca.fr